

Data Protection Impact Assessment (DPIA) — TOMYO (voor klanten)

Datum: 18-01-2026

Versie: 1.0

1. Samenvatting van de verwerking

- Verwerkingsverantwoordelijke: [Naam praktijk / logopedist]
- Verwerker: Encover BV (TOMYO) — contact: niels@encover.be (DPO: Niels Meeus)
- Doel: beheer van patiëntdossiers (intake, EPD, metingen, bilans), foto-opslag, Payne-mapping, communicatie (e-mail) en administratie.
- Rechtsgrondslag: uitvoering van medische behandeling / expliciete toestemming (selecteer en documenteer).
- Categorieën betrokkenen: patiënten (cliënten), praktijkmedewerkers.
- Categorieën persoonsgegevens: identificatie, contact, medische/gezondheidsgegevens, foto's/beeldmateriaal, Payne-mapping-coördinaten, authenticatie- en loggegevens.
- Overdrachten buiten EU/EEA: Ja — Postmark (e-mailadressen en e-mailinhoud). Verwerker heeft contractuele waarborgen (SCC of gelijkwaardig) en minimale data-uitwisseling met Postmark beperkt tot uitgaande e-mails; geen structurele opslag van volledige patiëntdossiers buiten EEA.

2. Beschrijving van gegevensstromen

- Invoer via web-UI → opgeslagen in database tabellen (epd., *m_metingen.*, *m_onderzoeken.*, *uploads/*).
- Uploads (foto's): opgeslagen op hostingprovider Combell (data EU/EEA) — gevoelig materiaal.
- E-mails via Postmark (API-key via secret store).
- Back-ups en logs opgeslagen conform hostingbeleid (versleuteld).

3. Beoordeling van noodzaak en proportionaliteit

- Noodzakelijkheid: verwerking is functioneel noodzakelijk voor diagnose, behandeling en dossiervoering.
- Proportionaliteit: alleen relevante gegevens verzamelen; anonimiseren waar mogelijk; minimale retentie.

4. Risicoanalyse (hoog-normatief)

- Risico A — Ongeautoriseerde toegang tot EPD/foto's: impact hoog, waarschijnlijkheid middel.
- Risico B — Ongeoorloofde exfiltratie/uploads gedeeld: impact hoog, waarschijnlijkheid laag/middel.
- Risico C — Onjuiste backdating (datumoverrides) zonder audit: impact middel, waarschijnlijkheid laag.

- Risico D — Geheime keys (env) gelekt: impact hoog, waarschijnlijkheid laag (mitigaties aanwezig).
 - Risico E — Ongepaste e-mailing van PHI: impact hoog, waarschijnlijkheid laag (mitigatie: geen PHI in e-mails).
5. Bestaande en aanbevolen mitigaties (technisch & organisatorisch)
- Secrets & configuratie:
 - Gebruik KMS/secret manager; tomyo.env buiten webroot met permissies 600.
 - Authenticatie & toegang:
 - RBAC, sterke wachtwoorden, MFA verplicht voor therapeut/administrator rollen.
 - Data-at-rest en transport:
 - TLS voor alle verbindingen; DB/filesystem encryptie van patiëntgegevens
 - Uploads & foto's:
 - Opslag buiten webroot; random filenames; strip EXIF; access control.
 - Back-ups:
 - Versleutelde back-ups, beperkte toegang, periodieke restore-test.
 - Operationeel:
 - Incident response procedure
 - DPA tussen praktijk en Encover BV ondertekend.
 - Juridisch/beleid:
 - Bewaartermijnen vastleggen (EPD 30 jaar) en opname in privacybeleid.
 - Minimale gegevensinvoer policy en patient consent flows.
6. Residueel risico en acceptatie
- Na voorgestelde mitigaties: residueel risico naar laag/middel voor de meeste scenario's.
7. Verwerkers & subverwerkers
- Verwerker: Encover BV (TOMYO) — niels@encover.be (DPO: Niels Meeus)
 - Subverwerkers: Postmark (e-mail, kan verwerking buiten EU/EEA doen voor uitgaande e-mails; dataoverdracht beperkt tot e-mailadressen en e-mailinhoud). Waarborgen: schriftelijke overeenkomst + EU Standard Contractual Clauses (of equivalente maatregelen).
 - Hosting: Combell (België, EU/EEA) — primair datacenter voor patiëntgegevens en uploads.
8. Data-retentie en verwijdering
- EPD / medische dossiers: 30 jaar na laatste contact (definitief bevestigd)

- Foto's: 30 jaar (of gelijk aan EPD)
- Logs/audit: 2 jaar

9. Rechten van betrokkenen & operationele maatregelen

- Mechanisme voor inzage/rectificatie/verwijdering: contact praktijk; Verwerker ondersteunt verzoeken.
- Procedures voor dataportability en bewaarverzoeken implementeren.
- Documenteer alle verzoeken en acties in audit-log.

10. Incident response en meldplicht

- Volg docs/Incident_Response_Procedure.md.
- Toezichthoudermelding binnen 72 uur indien hoog risico; praktijk (Verantwoordelijke) beslist over notificatie van betrokkenen.

11. Gegevensoverdracht en subverwerkers

- Verwerker: Encover BV (TOMYO) — niels@encover.be (DPO: Niels Meeus)
- Subverwerkers: Postmark (e-mail, kan verwerking buiten EU/EEA doen voor uitgaande e-mails; dataoverdracht beperkt tot e-mailadressen en e-mailinhoud). Waarborgen: schriftelijke overeenkomst + EU Standard Contractual Clauses (of equivalente maatregelen).
- Hosting: Combell (België, EU/EEA) — primair datacenter voor patiëntgegevens en uploads.

12. Data-retentie en verwijdering

- Retentie (praktijk kan aanpassen op aanvraag via mail):
 - EPD / medische dossiers: 30 jaar na laatste contact
 - Foto's: 30 jaar (of gelijk aan EPD)
 - Logs/audit: 2 jaar

13. Rechten van betrokkenen & operationele maatregelen

- Mechanisme voor inzage/rectificatie/verwijdering: contact praktijk; Verwerker ondersteunt verzoeken.
- Procedures voor dataportability en bewaarverzoeken implementeren.
- Documenteer alle verzoeken en acties in audit-log.

14. Incident response en meldplicht

- Volg docs/Incident_Response_Procedure.md.
- Toezichthoudermelding binnen 72 uur indien hoog risico; praktijk (Verantwoordelijke) beslist over notificatie van betrokkenen.

15. Audit, monitoring en review

- Jaarlijkse review van DPIA en technische maatregelen of bij significante wijziging.
- Periodieke pentests en vulnerability scans aanbevolen.

16. Contacten & rapportage

- Verwerker (incident owner): Niels Meeus — niels@encover.be
- Hosting: Combell support: <https://www.combell.com/>
- Subverwerker e-mail: Postmark support: <https://postmarkapp.com/>
- Toezichthouder (BE): Gegevensbeschermingsautoriteit — <https://www.gegevensbeschermingsautoriteit.be/>

17. Bijlagen (steeds op te vragen via niels@encover.be)

- Incident response procedure
- Data Protection Impact Assessment
- Technische controls inventaris
-

• **## Bijlage A – Gedetailleerde lijst van verwerkte velden (gebaseerd op codebase en views)**

-
- Algemeen:
 - - client_id / patient_id
 - - intake_id, meting_id, onderzoek_id, upload_id, sessie_id
 - - created_at, updated_at
 - - user_id (creator/editor)
-
- EPD / Identificatie:
 - - naam (encrypted)
 - - voornaam (encrypted)
 - - geboortedatum (encrypted)
 - - geslacht (encrypted)
 - - adres, postcode, woonplaats (encrypted)
 - - telefoonnummer(s) (encrypted)
 - - e-mailadres (encrypted)
 - - RSZ-gegevens (encrypted)
 - - nationaliteitsveld (indien aanwezig) (encrypted)
-
-
- Gebruikers & Authenticatie (praktijken en therapeuten):
 - - gebruikersnaam / displayname
 - - e-mail
 - - rol (eigenaar, administrator, superadministrator, therapeut, etc.)
 - - wachtwoord hash
 - - MFA status / tokens / last_login
 - - permissies
-

- Technische / Overige:
- - session_id, IP-adres (login metadata)
- ---
-
- **## Bijlage B – Aanbevolen bewaartermijnen (conform veelvoorkomende Belgische praktijk – bevestigen met juridisch advies)**
- - EPD / medische dossiers: 30 jaar na laatste contact
- - Foto's: gelijk aan EPD (30 jaar)
- - Logs / audit: 2 jaar (met mogelijkheid tot langer bewaren voor juridische redenen)